

Damien ROBERT

Researcher in cryptography

Libourne, France

+33 (0)6 66 56 25 49

+33 (0)5 40 00 21 56

✉ damien.robert@inria.fr

📄 www.normalesup.org/~robert/

👤 DamienRobert

French, Born in 1984



Research

List of publications: www.normalesup.org/~robert/pro/publications/, see also *the appendix*.

Work

- March 2012–Present Researcher, *Inria Bordeaux Sud-Ouest, Bordeaux*, Inria Team LFANT.
Elliptic curves, abelian varieties and algorithmic number theory applied to cryptography
- August 2011– February 2012 Researcher Engineer, *Microsoft Research, Redmond*, Team manager: Kristin Lauter.
Developing the Microsoft cryptographic library.
- October 2010– August 2011 Postdoc, *Inria Bordeaux Sud-Ouest, Bordeaux*, Team manager: Andreas Enge.
Genus 2 curves and complex multiplication.
- July 2010– September 2010 Microsoft Research Summer Internship, *Redmond, USA*, Mentor: Kristin Lauter.
Speeding up the CRT method in genus 2 for generating class polynomials

Education

- January 2007– June 2010 PhD Thesis, *University Henri Poincaré and Loria, Nancy*, Advisor: Guillaume Hanrot, Teaching Fellow (Moniteur) in Computer Science.
Theta functions and applications in cryptography. Defended July 23 2010.
- September– December 2006 Master of Science in Computer Science, *Paris*, Master Parisien de Recherche Informatique, (Inscription Pédagogique).
Courses in cryptography and algebraic number theory
- 2004–2006 Master of Science in Mathematics, *Paris VI, Paris VII, Paris XI, École Polytechnique*, Algebra and Geometry, With Honors (Courses: 19.88/20, Master Thesis: 18/20, Total: 18.94/20).
(Pedagogic inscription in 2004–2005.) Master Thesis on “Classification of complex reflexion groups”, Advisor: Michel Broué (Institut Henri Poincaré).
- 2004–2005 Agrégation in Mathematics, Nationwide competitive examination for recruiting teachers for undergraduate students, Rank 9.
- 2003–2007 École Normale Supérieure, *Paris*, Computer Science, Admitted after the French “Grandes Écoles” competitive examination, Rank 1.
- 2003–2006 Magistère in Mathematics (MMFAI), With Honors.
- 2003–2004 Bachelor of Science in Mathematics (L3–M1), With Honors (L3: 19/20, M1 Courses: 18.67/20, M1 Thesis: 14/20, M1 Total: 17/20).
Minor in Computer Science. Bachelor Thesis on « Clifford modules and K -theory », with Mehdi Tibouchi, advisor François Pierrot.

Experiences

- 2003 – 2006 **Computer Tutor**. Help students to use the school computers, organizations of workgroup on \LaTeX , Unix..., École Normale Supérieure, Paris.

2003 – 2006 Student administrator. Help the system administrators to maintain the school computers (on Solaris and FreeBSD), configuration of the user sessions, software installation, École Normale Supérieure, Paris.

Langages

French Native Speaker
English Fluent
German Basic

I have lived one year in Knoxville, Tennessee

Technical Skills

Programming C, JAVA, Ocaml, Perl, PHP, Ruby, Shell
Scientific Magma, Matlab, Pari, Sage
Web (X)HTML, CSS, Javascript

OS Linux (Archlinux)
VCS Git, Mercurial, Subversion
Typography Lua[®]TeX

Hobbies

Sport Juggling, Rock Climbing, Tennis.
Safety French First Aid Certificate
Other Driving license.

Scientific activities

Publications

- D. Lubicz and D. Robert. “Arithmetic on Abelian and Kummer Varieties”. In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: [10.1016/j.ffa.2016.01.009](https://doi.org/10.1016/j.ffa.2016.01.009). URL: <http://www.normalesup.org/~robert/pro/publications/articles/arithmetical.pdf>. HAL: [hal-01057467](https://hal.archives-ouvertes.fr/hal-01057467), eprint: 2014/493.
- D. Lubicz and D. Robert. “Computing separable isogenies in quasi-optimal time”. In: *LMS Journal of Computation and Mathematics* 18 (1 Feb. 2015), pp. 198–216. DOI: [10.1112/S146115701400045X](https://doi.org/10.1112/S146115701400045X). arXiv: 1402.3628. URL: <http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf>. HAL: [hal-00954895](https://hal.archives-ouvertes.fr/hal-00954895).
- D. Lubicz and D. Robert. “A generalisation of Miller’s algorithm and applications to pairing computations on abelian varieties”. In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: [10.1016/j.jsc.2014.08.001](https://doi.org/10.1016/j.jsc.2014.08.001). URL: <http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf>. HAL: [hal-00806923](https://hal.archives-ouvertes.fr/hal-00806923), eprint: 2013/192.
- R. Cosset and D. Robert. “An algorithm for computing (ℓ, ℓ) -isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2”. In: *Mathematics of Computation* 84.294 (Nov. 2015), pp. 1953–1975. DOI: [10.1090/S0025-5718-2014-02899-8](https://doi.org/10.1090/S0025-5718-2014-02899-8). URL: <http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf>. HAL: [hal-00578991](https://hal.archives-ouvertes.fr/hal-00578991), eprint: 2011/143.
- K. E. Lauter and D. Robert. “Improved CRT Algorithm for Class Polynomials in Genus 2”. In: *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Berkeley: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: [10.2140/obs.2013.1.437](https://doi.org/10.2140/obs.2013.1.437). URL: <http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf>. Slides: [2012-07-ANTS-SanDiego.pdf](https://www.normalesup.org/~robert/pro/publications/articles/2012-07-ANTS-SanDiego.pdf) (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA), HAL: [hal-00734450](https://hal.archives-ouvertes.fr/hal-00734450), eprint: 2012/443.
- D. Lubicz and D. Robert. “Computing isogenies between abelian varieties”. In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515. DOI: [10.1112/S0010437X12000243](https://doi.org/10.1112/S0010437X12000243). arXiv: 1001.2016 [math.AG]. URL: <http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf>. HAL: [hal-00446062](https://hal.archives-ouvertes.fr/hal-00446062).
- J.-C. Faugère, D. Lubicz, and D. Robert. “Computing modular correspondences for abelian varieties”. In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 248–277. DOI: [10.1016/j.jalgebra.2011.06.031](https://doi.org/10.1016/j.jalgebra.2011.06.031). arXiv: 0910.4668 [cs.SC]. URL: <http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf>. HAL: [hal-00426338](https://hal.archives-ouvertes.fr/hal-00426338).
- D. Lubicz and D. Robert. “Efficient pairing computation with theta functions”. In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer-Verlag, July 2010. DOI: [10.1007/978-3-642-14518-6_21](https://doi.org/10.1007/978-3-642-14518-6_21). URL: <http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf>. Slides: [2010-07-ANTS-Nancy.pdf](https://www.normalesup.org/~robert/pro/publications/articles/2010-07-ANTS-Nancy.pdf) (30min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy), HAL: [hal-00528944](https://hal.archives-ouvertes.fr/hal-00528944).

Preprints

- E. Milio and D. Robert. “Modular polynomials on Hilbert surfaces”. Sept. 2017. HAL: [hal-01520262](https://hal.archives-ouvertes.fr/hal-01520262).

- A. Dudeanu, jetchev, D. Robert, et al. “Cyclic Isogenies for Abelian Varieties with Real Multiplication”. Oct. 2017. HAL: [hal-01629829](#).

Reports

- [Andreas Enge, Damien Robert, Computing class polynomials in genus 2](#). DGA Report, April 2013.

PhD Thesis

- [Theta functions and cryptographic applications](#) (in French). PhD thesis in Computer Sciences, July 2010, Université Henri-Poincaré, Nancy. (Slides: [2010-07-Phd-Nancy.pdf](#) (1h, Nancy), TEL: [tel-00528942](#).)

Prizes

- February 2012 Received the second prize in Science for the [Lorraine Region PhD awards](#), Metz. ([Inria announcement](#))
- October 2011 Received the [Lorraine University PhD awards](#) in the domain of [IAEM](#) (Computer science, Mathematics, Electronic), Nancy. ([Photos of the ceremony](#))

Softwares

- [AVIsogenies](#) (Abelian Varieties and Isogenies), with [Gaëtan Bisson](#), [Romain Cosset](#). Magma package devoted to the computation of isogenies between abelian varieties, 2010. Free software (LGPLv2+), registered to APP (reference [IDDN.FR.001.440011.000.R.P.2010.-000.10000](#)). Latest version 0.6, released on 2012-11-28.

Teaching

- December 2015 Introduction to cryptology. Seminar on security of the Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun. [À quoi sert la cryptologie? Petit panorama des mathématiques de la cryptologie](#), [Introduction to cryptology: confidentiality, integrity, authenticity](#), [Modern cryptology: from public key cryptography to homomorphic encryption](#)
- September 2015 [The group structure of rational points of elliptic curves over a finite field](#) (3h). [Elliptic Curves Cryptography \(ECC 2015\) Summer School](#), Bordeaux. ([Exercices](#).)
- March 2015 [Algorithmic number theory and cryptology](#). One week courses for the École Mathématique Africaine, organised with support from the Centre International de Mathématiques Pures et Appliquées (CIMPA), Franceville, Gabon. [Introduction to the course](#), [Slides](#), [Examples](#) (X509, ssh, gpg)
- September 2011 [Isogenies and endomorphism rings of elliptic curves](#) (2h30). [ECC 2011 Summer School](#), Nancy.
- 2007 – 2010 Teaching Fellow (Moniteur) in Computer Science. Université Henri-Poincaré (Nancy).
 - Tutorials of the cryptography course (M1, 30h).
 - Course on Web technologies: HTML, CSS, PHP and MySQL (L1, 60h).
 - Tutorials of the OCaml programming course (L1, 120h).
- March 2004 – May 2004 [Corps quadratiques et groupes de classes](#). Workgroup organized with Mehdi Tibouchi, École Normale Supérieure, Paris.

Students

- November 2012 – December 2015 [Enea Milio](#), Isogenies between abelian surfaces, cosupervising with [Andreas Enge](#). Phd Thesis, Inria Bordeaux Sud-Ouest.

- 2014 Illaria Chillotti, Pairings over elliptic curves using isogenies. Master, Institut de Mathématiques de Bordeaux.
- 2013 Giulio Di Piazza, [Arithmetic on Jacobians of algebraic curves](#). Master, Institut de Mathématiques de Bordeaux.
- 2012 Ilaria Lovato, [Computing Modular Polynomials with Theta Functions](#), cosupervising with [Andreas Enge](#). Master, Institut de Mathématiques de Bordeaux.

Responsibilities

- December 2015 – Present Commission Consultative 25, Institut Mathématiques de Bordeaux.
- January 2015 – Present Commission Jeunes Chercheurs, Inria Bordeaux.
- 2014 – Present Jury of Mathematics agregation competition.
- June 2013 – Present Codirector of the team MACISA, inside the laboratory LIRIMA (Since September 2014; previously scientific adviser for the theme "Elliptic and hyperelliptic curves cryptography").
- October 2010 – Present Organisation of the [LFANT seminars](#).
- 2012 – 2016 Member of the ERC [Antics](#) (Algorithmic Number Theory in Computer Science).
- 2013 – 2016 Member of the Industrial ANR [Simpatic](#) (SIM and PAiring Theory for Information and Communications security).
- 2012 – 2015 Member of the ANR [Peace](#) (Parameter spaces for Efficient Arithmetic and Curve security Evaluation).
- 2012 – Present [Member of the LabEx CPU](#) (Numerical certification and reliability).
- 2009 – 2012 Member of the ANR [Chic](#) (Hyperelliptic curves, isogenies and point counting).

Comitees

- December 2015 [CRI 2015](#), Yaoundé, Cameroun. Scientific Comitee.
- December 2015 [Asiacrypt 2015](#), Auckland. Scientific Comitee.
- September 2015 [Elliptic Curves Cryptography \(ECC 2015\)](#), Bordeaux. Organisation Comitee, Scientific Comitee.
- August 2013 [Selected Area in Cryptography \(SAC 2013\)](#), Simon Fraser University, Canada. Scientific Comitee.

Invited Speaker

- [Isogenies, Polarisation and Real Multiplication](#) (1h). Journées C2 Codage et Cryptographie, October 2015, La Londe-Les-Maures.
- [Isogenies, Polarisation and Real Multiplication](#) (1h). [Modular Forms and Curves of Low Genus: Computational Aspects](#), September 2015, ICERM, Providence, USA. ([Long version](#).)
- [Optimal pairings on abelian varieties](#) (1h). [Elliptic Curves Cryptography \(ECC 2014\)](#), October 2014, Chennai, India.
- [Isogenies between abelian varieties \(Notes\)](#) (1h). ANR [Peace](#) conference [Effective moduli spaces and applications to cryptography](#), June 2014, Rennes.
- [Pairings on abelian varieties and the Discrete Logarithm Problem](#) (1h). Discrete Logarithm Problem Conference [DLP 2014](#), May 2014, Ascona, Suisse.
- [Computing optimal pairings on abelian varieties with theta functions](#) (1h). [Geometry and Cryptography \(Geocrypt 2011\)](#), June 2011, Bastia.

- Generalizing Vélu's formulas and some applications (1h). Elliptic Curves Cryptography (ECC 2010), 25 year anniversary of elliptic curves computation, October 2010, Redmond, USA. (Video link.)
- A Vélu's like formula for computing isogenies on Abelian Varieties (1h). Conférence Algorithmique et Arithmétique avec applications à la cryptographie, May 2010, Moscow, Russia.

Talks

- Arithmetic on Abelian and Kummer varieties (2x1h). INRIA Team LFANT seminar, May 2015, Bordeaux. On blackboard, notes.
- Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties (45min). École Mathématique Africaine, March 2015, Université de Masuku, Franceville, Gabon.
- Arithmetic on Abelian and Kummer varieties (1h). Number Theory Seminar, December 2014, Caen. On blackboard, notes.
- Isogeny graphs in dimension 2 (1h). Cryptography Seminar, December 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (1h). Number Theory Seminar, April 2014, Institut Fourier, Grenoble. On blackboard, notes.
- Arithmetic on abelian varieties and related topics (1h). Seminar in Coding Theory and Cryptography of the University of Zurich and the University of Neuchâtel, March 2014, Neuchâtel, Suisse.
- Computing optimal pairings on abelian varieties with theta functions (1h). Industrial ANR Simpatc meeting, January 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (30min). ANR Peace meeting, December 2013, Rennes.
- On isogenies and polarisations (1h). LFANT Seminar, November 2013, Bordeaux.
- On isogenies and polarisations (30min). Geometry and Cryptography (Geocrypt 2013), October 2013, Tahiti.
- On isogenies between abelian varieties (45min). Microsoft Research, August 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (1h). Microsoft Research, August 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (30min). Arithmetic Geometry Cryptography and Coding Theory (AGCT 14), June 2013, Luminy, Marseille.
- Computing optimal pairings on abelian varieties with theta functions (1h). Laca, May 2013, Lausanne.
- Computing optimal pairings on abelian varieties with theta functions (1h). CCIS seminar, April 2013, Grenoble.
- Computing cyclic isogenies using real multiplication (Notes) (1h). ANR Peace meeting, April 2013, Paris.
- Computing rational isogenies from the equations of the kernel (30min). ANR Peace meeting, November 2012, Paris.
- Improved CRT Algorithm for class polynomials in genus 2 (1h). Microsoft Research, August 2012, Redmond, USA.
- About the CRT method to compute class polynomials in dimension 2 (1h). INRIA Team LFANT seminar, May 2012, Bordeaux.
- Algorithms on abelian varieties for cryptography (1h). Caen's Cryptographic Seminar, March 2012, Caen.

- Algorithms on abelian varieties for cryptography (2h). INRIA Team Grace Seminar, January 2012, LIX, École Polytechnique, Paris.
- Algorithms on abelian varieties for cryptography (1h). Butte aux cailles Seminar, January 2012, Télécom ParisTech, Paris.
- Public key cryptography with abelian varieties: results and challenges (1h). ARITH Seminar, November 2011, Montpellier.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire de théorie des nombres, September 2011, Bordeaux.
- About the CRT method to compute class polynomials in dimension 2 (1h). Journées C2 Codage et Cryptographie, April 2011, Oléron.
- Cryptology, elliptic curves and number theory (1h). Number Theory PhD Students' seminar, March 2011, Bordeaux.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire Arithmétique et Théorie de l'Information, February 2011, Université Méditerranée, Marseille.
- Abelian varieties, theta functions and cryptography (1h30). PhD Students' seminar, February 2011, Université Méditerranée, Marseille.
- Computing isogenies and applications in cryptography (1h). Cryptology seminar, January 2011, Université Versailles Saint-Quentin, Versailles.
- Computing isogenies and applications in cryptography (1h). Minalogic cryptology seminar, January 2011, Grenoble.
- Abelian varieties, theta functions and cryptography (40min+40min). Algorithmics of L-functions workshop, December 2010, Bordeaux. Part 1 on blackboard.
- On the CRT method to compute class polynomials in genus 2 (30min). ANR Chic, December 2010, Paris.
- Generalizing Vélu's formulas and some applications (1h). TANC Seminar, November 2010, LIX, École Polytechnique, Paris.
- Speeding up the CRT method to compute class polynomials in genus 2 (1h). Microsoft Research, September 2010, Redmond, USA.
- Abelian varieties, Theta functions and cryptography (30min). Microsoft Research, July 2010, Redmond, USA.
- Arithmétique rapide avec les fonctions thêta (20min). ANR Chic, June 2010, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire de théorie des nombres, February 2010, Bordeaux.
- Calcul de pairing avec les fonctions thêta (1h). LFANT Cryptographic Seminar, February 2010, Bordeaux.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire Arithmétique et Théorie de l'Information, November 2009, Marseille.
- An efficient computation of the commutator pairing (20min). ANR Chic, October 2009, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (40min). ANR Chic, October 2009, Paris.
- Computing isogenies of small degrees on abelian varieties (20min). Journées d'arithmétiques 2009, July 2009, Saint-Etienne.
- Computing isogenies of small degrees on abelian varieties (1h). Séminaire de cryptographie, April 2009, Rennes.

- **Abelian varieties and isogenies** (30min). **Tsukuba Cryptographic Seminar**, November 2008, Tsukuba, Japan.

Vulgarization

- March 2015 Discussion with the public about the movie *Imitation Game* on the role of Alain Turing in Computer Science and Cryptography, Bordeaux.
- April 2014 **Algorithmic number theory and cryptography** (30min). Team presentation for the director of Inria Bordeaux, Inria Bordeaux.
- December 2013 **Algorithmic number theory and cryptography** (30min). Presentation of my research themes to the Inria Bordeaux Scientific committee, Inria Bordeaux.
- 2012 – 2013 Writing articles for **Sonews**, the internal paper of the research center Inria Bordeaux., Bordeaux.
- April 2013 **Petit panorama des mathématiques de la cryptologie**. Presentation for the students in **Mines de Nancy**, Labri, Bordeaux.
- February 2012 **Panorama de la cryptographie sur les courbes elliptiques**. Lorraine Phd **prize ceremony**, Conseil général de Lorraine, Metz. [More info](#).
- June 2011 Students meeting **Aquitec 2011**, Bordeaux.

Activities Slides

- May 2015 **MACISA — Mathematics applied to cryptology and information security in Africa** (30 min). Lirima team leaders meeting, Saint-Louis, Sénégal.
- September 2014 **MACISA — Mathematics applied to cryptology and information security in Africa** (30 min). Evaluation seminar of the Lirima laboratory, Paris.
- August 2014 **Bordeaux 2016: A canonical choice for ANTS XII** (15 min). Presentation to host ANTS XII in Bordeaux, GyeongJu, Korea.
- September 2013 **MACISA — Mathematics applied to cryptology and information security in Africa** (30min). Presentation of the MACISA team for the **Lirima** days, Rabat, Maroc.

Patents

- **Kristin Lauter, Damien Robert, Computing genus 2 curves using general isogenies**. May 2014.

Foreign stays and conferences attended

- December 2015 Seminar on security of the Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun.
- October 2015 Journées C2 Codage et Cryptographie, La Londe-Les-Maures.
- September 2015 **Elliptic Curves Cryptography (ECC 2015) Summer School**, Bordeaux.
- September 2015 **Modular Forms and Curves of Low Genus: Computational Aspects**, ICERM, Providence, USA.
 - May 2015 Lirima team leaders meeting, Saint-Louis, Sénégal.
- March 2015 École Mathématique Africaine, Franceville, Gabon.
- October 2014 **Elliptic Curves Cryptography (ECC 2014)**, Chennai, India.
- September 2014 Evaluation seminar of the Lirima laboratory, Paris.
 - August 2014 International Algorithmic Number Theory Symposium (ANTS-XI), GyeongJu, Korea.
 - August 2014 International Congress of Mathematicians (ICM 2014), Seoul, Korea.
- June 2014 **ANR Peace** conference **Effective moduli spaces and applications to cryptography**, Rennes.

- May 2014 Discrete Logarithm Problem Conference **DLP 2014**, Ascona, Suisse.
- March 2014 Journées C2 Codage et Cryptographie, Grenoble.
- October 2013 **Geometry and Cryptography (Geocrypt 2013)**, Tahiti.
- September 2013 Journées du Lirima, Rabat, Maroc.
- August 2013 One week visit to Microsoft Research, Redmond, USA.
- August 2013 **Selected Area in Cryptography (SAC 2013)**, Simon Fraser University, Canada.
- June 2013 **Arithmetic Geometry Cryptography and Coding Theory (AGCT 14)**, Luminy, Marseille.
- May 2013 One week visit to EPFL, Lausanne.
- January 2013 Pari/GT Workshop, Bordeaux.
- October 2012 Journées C2 Codage et Cryptographie, Dinard.
- August 2012 One week visit to Microsoft Research, Redmond, USA.
- July 2012 **International Algorithmic Number Theory Symposium (ANTS-X)**, San Diego, USA.
- September 2011 Elliptic Curves Cryptography (ECC 2011) and Summer School, Nancy.
- June 2011 **Geometry and Cryptography (Geocrypt 2011)**, Bastia.
- April 2011 Journées C2 Codage et Cryptographie, Oléron.
- December 2010 **Algorithmics of L-functions** workshop, Bordeaux.
- October 2010 **Elliptic Curves Cryptography (ECC 2010)**, 25 year anniversary of elliptic curves computation, Redmond, USA.
- July 2010 – September 2010 Three month Microsoft Research Internship in the cryptographic team to work on genus 2 class polynomials with Kristin Lauter, Redmond, USA.
- July 2010 **International Algorithmic Number Theory Symposium (ANTS-IX)**, Nancy.
- May 2010 **Conférence Algorithmique et Arithmétique avec applications à la cryptographie**, Moscow, Russia.
- October 2009 Elliptic Curves Cryptography (ECC 2009), Calgary.
- July 2009 **Journées d'arithmétiques 2009**, Saint-Etienne.
- March 2009 Arithmetic Geometry Cryptography and Coding Theory (AGCT), Luminy.
- November 2008 Three weeks visit at Tsukuba University in the team of professor Okamoto to work on pairings, Tokyo.
- October 2008 CADO workshop on integer factorisation, Nancy.
- July 2008 International Algorithmic Number Theory Symposium (ANTS-VIII), Banff, Canada.
- June 2008 Crypto week, LIX, Saclay..
- April 2008 École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Marseille.
- June 2007 LLL+25, Caen.
- March 2007 École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Nancy.
- February 2007 Journées nationales du calcul formel, Luminy.
- April 2006 Théorie géométrique et cohomologie des groupes: rigidité et déformations (Summer school), Luminy.